UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632

27871 7590 04/13/2006

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/025,924	VANSTONE ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *1-14* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on March 3, 2006. Claims 1 and 9 have been amended. Claims 1-14 are pending.

Claim Rejections - 35 USC § 112

2. In view of the amendment filed March 3, 2006, the Examiner withdraws the rejection of claim 1 under 35 USC 112.

Response to Arguments

3. Applicant's arguments filed March 3, 2006 have been fully considered but they are not persuasive. In response to the arguments concerning the previously rejected claims, the following comments are made:

The applicant argued Matyas does not teach, "performing a hash". The Examiner disagrees. Matyas teaches generating a seed value and hashing each of these seed values with SHA-1 to produce corresponding hash values. Therefore, Matyas teaches generating a seed and generating hash value by performing a hash function on the seed value. (Col. 5, line 65- Col. 6, line 8). In addition, Matyas further disclose the seed values are also kept secret. (Col. 6, line 24)

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention

where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to a person having ordinary skill in the art in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed. Matyas (Col. 7, lines 5-6) This way, further protection is given to the generated key.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "recognize minimize the bias in selection of k and use this bias not provide any steps to avoid the bias") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, Schneier teaches generating a seed value and determining if it is less than order q and Matyas teaches generating a seed value and performing a hash. Therefore, the combination of Schneier and Matyas teaches the limitations of claim 1.

Therefore, all the elements of the claims limitation are explicitly or implicitly or inherently suggested and disclosed by the combination of the references on the record and the previous rejection remains valid unless and otherwise the Applicant added a specific limitation in to the present independent claims, to overcome the rejection without introducing a new matter.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-2, 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Matyas, Jr. et al. (hereinafter Matyas) United States Letter Patent Number 6,307,938.

As per claim 1:

Schneier teaches a method of generating a key over a group of order q, said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

accepting said output for use as a key if the value thereof is less than said prime number q; (Page 487, lines 12-15) and

rejecting said output as a key if said value is not less than said order q. (Page 487, line 11)

In addition, Schneier further discloses performing a hash function (Page 487, lines 7-8; Page 489, lines 17-18) and determining whether a random number is less than q. (Page 487, line 11; ...k less than q)

Schneier does not explicitly disclose a method of performing a hash function on seed number to provide an output and determining whether said output is less than said prime number q.

Matyas in analogous art, however, discloses a method of performing a hash of each of seed values with SHA-1 to produce hash values; (Col. 6, lines 7-9) and generating seed involving a test to ensure that it falls within a specified range of allowed values and until it satisfies primality test. (Col. 6, line 65-Col. 8, line 35)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method of performing a hash function on seed number to provide an output and determining whether said output is less than said prime number q. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Matyas (Col. 7, lines 5-6) in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed.

As per claim 2:

The combination of Schneier and Matyas teach all the subject matter as discussed above. In addition, Schneier further discloses a method wherein another seed value is generated by said random number generator if said output is rejected. (Page 487, line 11; Page 489, line 22)

As per claim 4:

The combination of Schneier and Matyas teach all the subject matter as discussed above. In addition, Schneier discloses a method wherein said key is used for generation of a public key. (Page 487, lines 8-15; Page 488, line 3-8)

As per claim 5:

The combination of Schneier and Matyas teach all the subject matter as discussed above. In addition, Schneier further discloses a method wherein said order q is prime number represented by a bit string of predetermined length l. (Page 487, line 1 and Page 488, line 5)

6. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Matyas, Jr. et al. (hereinafter Matyas) United States Letter Patent Number 6,307,938 and further in view of Backal United States Letter Patent Number 6,219,421.

As per claim 7:

The combination of Schneier and Matyas teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash

function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

Backal in analogous art, however, disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. (Col. 5, lines 61-67)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method of wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 8:

The combination of Schneier, Matyas and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein said step of incrementing includes a further step of adding a particular value to said seed value. (Col. 5, lines 61-67)

As per claim 9:

Schneier teaches a method of generating a key over a group of order q, said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

accepting said new output as a key k if said new output has a value less than order q; (Page 487, line 11; ...k less than q) and

rejecting said new output as a key if said new output has a value less than order q . (Page 487, line 11)

In addition, Schneier further discloses performing a hash function (Page 487, lines 7-8; Page 489, lines 17-18) and determining whether a random number is less than q. (Page 487, line 11; ...k less than q)

Schneier does not explicitly disclose a method of performing a hash function on seed number to provide an output; determining whether said output is less than said prime number q; incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q.

Matyas in analogous art, however, discloses a method of performing a hash of each of seed values with SHA-1 to produce hash values; (Col. 6, lines 7-9) and generating seed involving a test to ensure that it falls within a specified range of allowed values and until it satisfies primality test. (Col. 6, line 65-Col. 8, line 35)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method of performing a hash function on seed number to provide an output and determining whether said output is less than said prime number q. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Matyas (Col. 7, lines 5-6) in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed.

Both references do not explicitly disclose incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q.

Backal in analogous art, however, disclose a method of

incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; (Col. 5, lines 61-67) and

combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q; (Col. 5, lines 54-60)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and

Matyas to include a method of incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order q. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 10:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said new output a new seed value is generated by said random number generator. (Page 487, line 11; Page 489, line 22)

As per claim 11:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained. (Col. 5, lines 61-67)

As per claim 12:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein a bit string greater than a predetermined length l is obtained and an l bit string selected therefrom for comparison with said order q. (Page 487, line 1 and Page 488, line 5)

As per claim 13:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said bit string of predetermined length l, a further l bit string is selected. (Page 487, line 1 and Page 488, line 5)

7. Claims 3 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Matyas, Jr. et al. (hereinafter Matyas) United States Letter Patent Number 6,307,938 in view of Nel et al. (hereinafter Nel) "Generation of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 3:

The combination of Schneier and Matyas teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein the step of accepting said output as a key includes a further step of storing said key.

Nel in analogous art, however, discloses a method wherein the step of accepting said output as a key includes a further step of storing said key. (Page 10, Col. 1, lines 3-4)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method wherein the step of accepting said output as a key includes a further step of storing said key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to be able to reuse the key and also to perform auditing on the key generation process.

As per claim 6:

The combination of Schneier, Matyas and Nel teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said output from said hash function is a bit string of predetermined length L.

Nel in analogous art, however, discloses a method wherein said output from said hash function is a bit string of predetermined length L. (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method wherein said output from said hash function is a bit string of predetermined length L. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel et al. (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.

8. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Backal United States Letter Patent

Number 6,219,421 and further in view of Nel et al. (hereinafter Nel) "Generatiion of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 14:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. Both references do not explicitly disclose method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length l.

Nel in analogous art, however, discloses a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length l. (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length l. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
4/4/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER